piratenpartei
www.piratenpartei.ch

Piratenpartei Schweiz
1337 Vallorbe

www.piratenpartei.ch

Positionspapier „Überwachung“

Zusammenfassung

Die Angst vor internationalem Terrorismus lässt Sicherheit vor Freiheit als wichtigstes Gut erscheinen – und viele fälschlicherweise in der Verteidigung der Freiheit verstummen. Ein Wildwuchs von Kameras und eine willkürliche Ausweitung von Überwachung beschneidet unser Grundrecht auf Privatsphäre, ist aber kaum zielführend. Massnahmen zur Erhöhung der öffentlichen Sicherheit müssen aufgrund von Statistiken und Fakten ergriffen werden. Überwachung muss sparsam und zielgerichtet eingesetzt werden und darf die Freiheit von uns allem nicht nur um des Aktionismus Willens einschränken. Menschliche Präsenz ist wann immer möglich einer Kamera vorzuziehen. Überwachung und Datenbanken können keine Taten verhindern!

Forderungen

1. Die Organe der repressiven und präventiven Überwachung müssen institutionell getrennt sein.
2. Der Datenaustausch zwischen den Organen der Prävention und Repression ist strikt zu reglementieren.
3. Repressive Überwachung bedarf eines hohen Masses an rechtsstaatlicher Kontrolle. Strikte Regeln müssen eingehalten und kontrolliert werden.
4. Die Privatsphäre ist grundsätzlich ein schutzwürdiges Gut und der Sicherheit gleich zu stellen.

Autoren:

- Michael Gregr, michael.gregr@piratenpartei.ch
- Pat Mächler, patrick.maechler@piratenpartei.ch
- Denis Simonet, denis.simonet@piratenpartei.ch

Inhaltsverzeichnis

Einleitung

> «They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety.»[1]
>
> *Benjamin Franklin (1706-1790), US-amerikanischer Staatsmann, Naturwissenschaftler und Schriftsteller.*

Durch den überwältigenden Erfolg des Internets und die fortwährende Weiterentwicklung unserer Technologien werden die bewährte Ordnung, das politische System und die Prinzipien der Rechtsstaatlichkeit gleichermassen auf den Prüfstand gestellt. So vielfältig die neuen Möglichkeiten sind, so verlockend ist es auch, sie für fragwürdige Zwecke einzusetzen. Besonders gefährlich ist das Verlangen nach mehr Überwachung, die heute in noch nie da gewesenem Umfang möglich ist. Das Streben nach Sicherheit lässt vergessen, wofür unsere Vorfahren einst gekämpft haben. Die Freiheit ist unser wichtigstes Gut. Sie muss sorgfältig und umsichtig behandelt werden!

1 William Temple Franklin (Hrsg.) (1818): *Memoirs of the life and writings of Benjamin Franklin,* Vol. 1, T.S. Manning, Philadelphia: S. 333-334.

Allgemeines zur Überwachung und Datenerhebung

Grundprinzipien des Datenschutzes und der Privatsphäre

Artikel 4 des Schweizer Datenschutzgesetzes[2] (DSG) definiert die Grundsätze nach denen Personendaten bearbeitet werden dürfen und geht unter anderem auf eine Konvention des Europarates zurück[3].

Der Schutz der Privatsphäre ist in Artikel 13 der Schweizer Bundesverfassung[4] folgendermassen vorgeschrieben:

1. Jede Person hat Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs.
2. Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.

Die 3 Grundprinzipien, nach denen Personendaten überhaupt erhoben und verarbeitet werden dürfen, sind namentlich die

- Rechtmässigkeit,
- Verhältnismässigkeit,
- und Zweckbindung.

Unabhängig von weitergehenden Problemen, die sich durch Überwachungsmöglichkeiten ergeben können, müssen diese Prinzipien immer angewandt werden, um die Gefahr einer Überwachungsgesellschaft abzuwenden.

2 http://www.admin.ch/ch/d/sr/235_1/a4.html

3 http://conventions.coe.int/Treaty/ger/Treaties/Html/108.htm

4 http://www.admin.ch/ch/d/sr/101/a13.html

Relevante Bundesgesetze

Es gibt verschiedene Bundesgesetze, die Überwachung regeln[5].

Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit (BWIS)

Dieses Gesetz[6] ist seit dem 21. März 1997 in Kraft. Sein Zweck ist die «Sicherung der demokratischen und rechtsstaatlichen Grundlagen der Schweiz sowie der Schutz der Freiheitsrechte ihrer Bevölkerung.» Es geht um vorbeugende Massnahmen, «um frühzeitig Gefährdungen durch Terrorismus, verbotenen Nachrichtendienst, gewalttätigen Extremismus und Gewalt anlässlich von Sportveranstaltungen zu erkennen und zu bekämpfen.» Die Legitimierung der umstrittenen Hooligandatenbank «HOOGAN» ist Bestandteil dieses Gesetzes.

Bundesgesetz über Massnahmen zur Wahrung der inneren Sicherheit II (BWIS II)

BWIS II[7] (im Entwurfstatus) soll dem Nachrichtendienst des Bundes (Geheimdienst) weitreichende Möglichkeiten an verdachtsunabhängiger Überwachung geben. Wir lehnen diese Vorlage ab - Überwachung muss einer demokratisch legitimierten Kontrolle unterliegen und darf nicht allein dem Gutdünken von Ämtern überlassen werden.

Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF)

Dieses Gesetz[8] regelt seit dem 6. Oktober 2000 die Überwachung des Post- und Fernmeldeverkehrs im Rahmen der Strafverfolgung sowie der Suche und Rettung vermisster Personen. Inhalte dieses Gesetzes sind unter anderem die Pflicht der Internetanbieter, Randdaten über IP-Adressen zu sammeln oder Ortungen von Mobiltelefonen durch zu führen. BÜPF betraut das zuständige Amt, genannt ÜPF, mit Rechten und Pflichten. Mit einer Revision soll die Überwachung des gesamten Internetverkehrs in Echtzeit eingeführt und die Dauer für die Speicherpflicht von Randdaten erhöht werden. Wir lehnen diese Ausweitung ab und fordern Statistiken und Analysen der Wirksamkeit der bestehenden Massnahmen. Sollte ein relevanter Zusammenhang zwischen bestimmten Massnahmen und dem Ermittlungserfolg bestehen, sind die Möglichkeiten und Fristen auf das absolute Minimum zu beschränken und als abschliessende Aufzählungen zu betrachten.

5 http://www.digitale-gesellschaft.ch/ueberwachung/

6 http://www.admin.ch/ch/d/sr/120/index.html

7 http://www.fedpol.admin.ch/fedpol/de/home/dokumentation/medieninformationen/2007/ref_2007-06-15.html

8 http://www.admin.ch/ch/d/sr/c780_1.html

Forderungen

Repression oder Prävention?

Forderungen:

- Zwischen den Organen der repressiven und präventiven Überwachung braucht es eine institutionelle Trennung.
- Der Datenaustausch zwischen den Organen der Prävention und Repression ist strikt zu reglementieren.
- Repressive Überwachung bedarf eines hohen Masses an rechtsstaatlicher Kontrolle. Strikte Regeln müssen eingehalten und kontrolliert werden.

Der Begriff «Überwachung» ist negativ belegt und wird meist nur im Zusammenhang mit dem Eindringen in die Privatsphäre eines Beobachteten verstanden. Überwachung kann jedoch mehr bedeuten und genauso gibt es verschiedene Anwendungen von Überwachung, die nicht alle gleich zu werten sind. Es ist zwischen repressiver und präventiver Überwachung zu unterscheiden. Um diese Unterscheidung zu verstehen, müssen die Konzepte von Repression und Prävention kurz erklärt werden. Beiden ist gleich, dass sie gesellschaftlich unerwünschte Ereignisse oder Handlungen verhindern sollen. Dies kann ein krimineller Akt aber auch ein unbeabsichtigter Unfall sein. Repression setzt nach einem Ereignis ein, um weitere direkte oder indirekte Folgeereignisse zu verhindern. Prävention setzt vor einem möglichen Ereignis ein – sie bewirkt, dass es nicht zu diesem kommt oder die Auswirkungen wenigstens nicht allzu gravierend sind. Auch wenn häufig gesagt wird, dass Repression präventiven Charakter hat (Stichwort Abschreckung), so trifft das nicht auf diese Unterscheidung zu. Das wird deutlich, wenn man sich die Formen vergegenwärtigt, wie uns Repression und Prävention im täglichen Leben begegnet. Repression begegnet uns in Form von Strafen, während Prävention die Gestalt von Hilfeleistungen annimmt.

Repressive Überwachung

Auf den Bereich der Überwachung angewendet, bedeutet dies, dass alle Formen von Überwachung, die dazu dienen, bereits geschehene Handlungen oder Ereignisse strafrechtlich zu verfolgen, als repressive Überwachung bezeichnet werden. Die Daten von Überwachungsinstallationen diesen Typs werden konsequenter Weise zur späteren Verwendung aufgezeichnet, weil sie erst nach dem Ereignis Verwendung finden. Repressive Überwachung bedarf eines hohen Masses an rechtsstaatlicher Kontrolle. Strikte Regeln müssen eingehalten und kontrolliert werden.

Präventive Überwachung

Überwachung, die *nicht* das Ziel verfolgt, Handlungen oder Ereignisse strafrechtlich zu verfolgen, sondern eine Intervention ermöglichen soll, die Handlungen und Ereignisse vor ihren eintreten verhindert, ist als präventive Überwachung zu bezeichnen. Daten aus Installationen diesen Typs müssen nicht zwangsläufig aufgezeichnet werden, weil die Verwendung nach dem Ereignis nicht primärer Zweck ist. Es kann jedoch sinnvoll sein, auch diese Daten aufzuzeichnen, um die Interventionsmechanismen durch Auswertungen zu verbessern. Jedoch muss die Verwendung zur Strafverfolgung ausgeschlossen sein. Präventive Überwachung bedarf keiner so hohen rechtsstaatlichen Kontrolle wie die repressive Überwachung. Die strikte institutionelle Trennung von Repression und Prävention ist zu gewährleisten.

Institutionelle Trennung von Repression und Prävention

Unter einer institutioneller Trennung ist die organisatorische Unabhängigkeit von zwei oder mehr Organen zu verstehen, um Interessenkonflikte zu verhindern. Im alltäglichen Leben schliessen sich Repression und Prävention gegenseitig aus; nur in der Theorie kann unter einiger argumentativer Verrenkung dargelegt werden, dass eine Strafe als Hilfeleistung an die Allgemeinheit zu verstehen ist, mit dem Ziel zukünftige Straftaten zu verhindern. Eine Strafe ist auf die Aversion der betroffenen Personen angewiesen; man muss Strafen nicht bekommen wollen, sonst wirken sie nicht. Hilfeleistungen hingegen müssen von der hilfebedürftigen Person angenommen werden, damit sie effektiv sind. Ein und dieselbe Person (bzw. ein und dasselbe Organ) kann also nicht zugleich repressiv und präventiv wirken. Z.B. kann die Hilfeleistung einer Drogenberatung nur effektiv sein, wenn der Hilfesuchende nicht fürchten muss, dass das vertrauliche Gespräch den Strafverfolgungsbehörden zu Kenntnis gebracht wird.

Auf das Thema der Überwachung angewendet, bedeutet institutionelle Trennung, dass repressive und präventive Überwachung nicht vom gleichen Organ durchgeführt werden dürfen, weil sonst ein Interessenkonflikt besteht. Präventive Überwachung will Ereignisse vor ihrem Eintreten verhindern, während repressive Überwachung sie beobachten will. Präventive Überwachung darf deshalb nicht Teil der Organisation der Strafverfolgungsbehörden sein. Viel mehr muss dafür eine eigenes staatliches Organ geschaffen werden, das den Notwendigkeiten von Prävention Rechnung trägt. Der Datenaustausch zwischen den Instituten der Prävention und Repression ist strikt zu reglementieren, z.B. durch eine richterliche Kontrolle. Obwohl ein Verbot des Datenaustausches theoretisch wünschenswert wäre, ist er praktisch nicht komplett durchführbar, denn die Aufklärung von Schwerverbrechen kann nicht ultimativ hinter dem Datenschutz zurückstehen.

Repression - Abschreckung - Prävention

Zum Stichwort Abschreckung, das häufig zur Rechtfertigung von exzessiver Anwendung von repressiver Überwachung herangezogen wird, bedarf es noch einiger Worte. Das Konzept der Abschreckung geht davon aus, dass die Furcht vor Strafe effektiv die Zahl der Straftaten senkt, je höher das Strafmass und die

Wahrscheinlichkeit erwischt zu werden. Der Streit über die Effektivität von Abschreckung ist endlos und die Befürworter lassen sich auch nicht von internationalen Vergleichsstudien überzeugen, die keinen Zusammenhang von Strafmass und Straftaten aufzeigen können. Viel mehr wird argumentiert, dass Überwachung die Effektivität von Strafverfolgung erhöht, weil die Wahrscheinlichkeit einen Straftäter zu überführen grösser ist - und damit steige die Abschreckung. Dieser Argumentation liegt jedoch ein Denkfehler zu Grunde. Abschreckung durch Überwachung funktioniert nur, wenn der Straftäter sich der erhöhten Überwachung bewusst ist. Repressive Überwachung ist aber nur wirkungsvoll, wenn der Straftäter sich ihr nicht bewusst ist, sonst verlagert sich nur der Tatort. Repressive Überwachung führt damit zu einer lokalen Verschiebung der Straftaten, je abschreckender sie wirkt. Effektiv hat sie nur eine senkende Wirkung auf Straftaten, wenn die repressive Überwachung konstant ausgedehnt und letztlich der gesamte öffentlich Raum überwacht wird. Wer also für Abschreckung durch Überwachung plädiert, will letztlich alle und jeden überwachen.

Datensparsamkeit und Informationspflicht

Forderungen:

- Datenerhebung und -bearbeitung muss begrenzt und kontrolliert sein. In diesem Kontext ist eine dezentrale Datenspeicherung zentralen Datenbanken vorzuziehen.
- Nur demokratisch legitimierte Kontrollmechanismen verhindern exzessive Datensammlungen. Eine judikative oder parlamentarische Genehmigung und Kontrolle muss deshalb zwingend vorhanden sein.
- Im Fall von Ermittlungen: Die Betroffenen Personen müssen im Nachhinein immer über die Datenerhebung informiert werden. Entsteht ihnen durch missbräuchliche Massnahmen ein Schaden, ist dieser in jedem Fall zu entschädigen.
- Auf Opt-Out-Datenbanken wie z.B. die Fahrzeughalterauskunft ist zu verzichten.

Ob biometrischer Pass, Hooligan-Datenbank oder die klassische Überwachungskamera - Daten werden überall gesammelt. Ideen für noch mehr Datenbanken gibt es viele, wie etwa Geräte in Autos und elektronische SBB-Fahrkarten, die das Fahrverhalten erfassen. Solche Datensammlungen bergen immer die Gefahr, in die falschen Hände zu geraten. Deshalb fordern wir, dass diese Grundsätze im Sinne der Datensparsamkeit eingehalten werden. Denn wo gar nicht erst Daten gesammelt werden, ist auch ein Missbrauch nicht möglich.

Videoüberwachung

Forderungen:

- Mit demokratischen Prozessen soll über Ausrichtung, technische Details und den Betrieb, insbesondere über Art und Dauer von Aufzeichnungen und über deren Auswertung entschieden werden.
- Videoüberwachung muss immer begründet und regelmässig auf die weitere Notwendigkeit überprüft werden.
- Keine flächendeckende Videoüberwachung des öffentlichen Raumes und eine restriktive Bewilligungspflicht im privaten Raum.

Der Entscheid, eine Kamera einzusetzen, muss im Auswahlverfahren zwischen verschiedenen Massnahmen gefällt werden. Das Aufstellen permanenter technischer Überwachungseinrichtungen, insbesondere für Bild- oder Tonaufnahmen, die den öffentlichen Grund überwachen können, muss stets durch die Legislative bewilligt werden. Wenn eine Kamera bewilligt wurde, ist eine regelmässige Überprüfung der weiteren Notwendigkeit der Kamera zwingend. Eine Kontingentierung von Kameras spart zusätzlich Kosten, weil sie dann nur dort eingesetzt werden, wo es tatsächlich notwendig ist und es keine andere Möglichkeit gibt.

Es gibt Alternativen zur systematischen Überwachung von neuralgischen Stellen. Möglich ist z.B. die gezielte Aktivierung von Kameras während Demonstrationen (im Sinne der Brandherdfrüherkennung). In Winterthur besteht der Plan, Fahrräder mit GPS-Sender als Köder aufzustellen. Wird das Fahrrad bewegt, handelt es sich höchstwahrscheinlich um einen Dieb. Diese beiden Überwachungsmodelle sind zielgerichtet und schränken die Privatsphäre der Allgemeinheit nicht unnötig ein. Mit den Fahrrad-Ködern kann sogar vollständig auf Videoüberwachung verzichtet werden!

Weiterführende Betrachtungen

Die Schattenseite von Datensammlungen

Am Dienstag, dem 14. Dezember 2010, ist es mal wieder passiert[9]. Ein unvorsichtiger Mitarbeiter der Informatik-Abteilung des Bezirks Mesa im US-Bundesstaat Colorado überliess die Daten von über 200'000 Personen der freien Wildbahn. Die Folge: Verdächtige Personen, Opfer von Verbrechen und Informanten des Bezirks konnten öffentlich eingesehen werden. Der Unfall geschah beim Kopieren einer Klartext-Datenbank des Polizeidepartements auf einen «sicheren» Server. Erst Monate später stellte sich heraus, dass die Akten dadurch für alle zugänglich im Web landeten. Natürlich konnten Verdächtige bequem verschwinden, Informanten fürchten um ihr Leben und Opfer sind der Gefahr weiterer Verbrechen ausgesetzt.

Dieses Datenleck ist kein Einzelfall. Wie «heise online» am 15. Dezember 2010 berichtete[10], verkaufte die Glücksburger Stadtverwaltung auf einem Flohmarkt versehentlich Festplatten mit Steuerbescheiden, Schreiben an Bürger, Dokumenten zu Genehmigungsverfahren, Konzessionen für Unternehmer, Gesprächsvermerken und Protokollen. «Cablegate» auf WikiLeaks ist ein weiteres Beispiel. Auf die 250'000 Depeschen hatten scheinbar etwa zwei Millionen Personen Zugriff[11]. Wen erstaunt es, dass diese Inhalte nun an die Öffentlichkeit gelangen?

Auch Sony wurde schon Opfer eines gewaltigen Datendiebstahls. Es gelang einem Eindringling, die 77 Millionen Benutzerprofile des Sony Playstation Networks zu beschaffen[12]. Aus dem Online-Spiele-Angebot Sony Online Entertainment wurden weitere 25 Millionen Profile kopiert[13]. Und Sony veröffentlicht etwas später aus Versehen selber noch einmal 2500 Datensätze[14]. Es folgten diverse weitere Hacks.

Diese dramatischen Beispiele illustrieren, wie gefährlich staatliche und zentrale Datenbanken sind. Die Liste solcher Vorfälle ist lang. Auch wenn uns oft versichert wird, wie sicher und geschützt diese sind – es gibt immer eine Schwachstelle und es passieren nun mal Fehler. Nicht zuletzt, weil das menschlich ist. Es liegt auf der Hand: Wir müssen diese Gefahr erkennen und auf Datensparsamkeit bestehen.

Vorratsdatenspeicherung

Wenn eine Straftat untersucht wird, die über das Internet begangen wurde, sind oft vor allem IP-Adressen bekannt. Diese haben isoliert allerdings keinen Wert. Die Ermittler behelfen sich deshalb mit den

9 http://arstechnica.com/security/news/2010/12/informants-suspects-outed-in-accidental-database-leak.ars

10 http://www.heise.de/newsticker/meldung/Bericht-Gluecksburger-Stadtverwaltung-verkauft-versehentlich-vertrauliche-Daten-1153224.html

11 http://www.dailytech.com/CDs+DVDs+ThumbDrives+Banned+from+SIPRNET+Under+Threat+of+CourtMartial/article20371.htm

12 http://www.denissimonet.ch/2011/04/27/bastler-verklagen-check-psn-absichern-oops/

13 http://www.rp-online.de/digitale/internet/2500-User-Daten-waren-im-Internet-abrufbar_aid_995501.html

14 http://www.golem.de/1105/83314.html

Randdaten, die jeder Internetprovider sammeln muss: Es wird Buch geführt, wann welcher Kunde mit welcher IP-Adresse wie lange unterwegs war. Diese Art der Datensammlung nennt sich Vorratsdatenspeicherung.

Es gibt heute einfache Möglichkeiten, Internetspuren zu verwischen. Mit TOR[15] (ein Anonymisierungsdienst) kann jeder die Herkunft verschleiern und mit GPG[16] den E-Mail-Verkehr verschlüsseln. Verbrecher verzichten wohl kaum darauf. So bringt auch eine Echtzeitüberwachung nichts und Randdaten sind nutzlos.

Selbst wenn der Anschluss mit diesen Methoden, mangels Täterkompetenz, ermittelt werden kann, ist Vorsicht geboten. Ein Haar alleine beweist keine Tat – auch dann nicht, wenn es auf der Tatwaffe war und per DNA-Abgleich einer Person zugeordnet wurde. Denn es könnte absichtlich hinterlegt worden sein. Genau so beweist eine IP-Adresse keineswegs, dass der Anschlussinhaber der Täter ist. Internetanschlüsse können auf verschiedene Arten verwendet und auch missbraucht werden. Offene WLANs, Trojaner oder auch die gemeinsame Verwendung des Zugangs mit dem Nachbarn sind Beispiele.

Es ist genau besehen nicht so klar, dass die Randdaten notwendig sind. Möglicherweise gab es noch nie den Fall, dass eine Rückverfolgung einer IP-Adresse zum Ermittlungserfolg führte. Statistiken würden Klarheit schaffen. Doch leider kennt das Bundesamt für Statistik «keine Zahlen zu den Vorgehen bei der Verbrechensaufklärung».

Eigentlich sollte es selbstverständlich sein, dass man vor der Erweiterung von Gesetzen und Verordnungen eine Analyse der aktuellen Situation durchführt. Ohne diese ist weder klar, wie wirkungsvoll die bisherigen Mittel sind, noch kann man ahnen, welche Auswirkungen eine allfällige Erweiterung hätte.

Angst und die Überwachungsspirale

Neue Überwachungsmethoden werden meist vor dem Hintergrund vorhandener Ängste eingeführt; insbesondere seit den Anschlägen vom 11. September lässt sich unbestritten ein sprunghafter Anstieg der politischen Forderungen nach Überwachung feststellen.

Die hohen Opferzahlen der Anschläge und die ausführliche Berichterstattung darüber machen verständlich, dass gewisse Ängste entstanden sind. Jedoch sind die Opferzahlen insgesamt gesehen gering: Das Risiko an einem internationalen Terroranschlag zu sterben, war sogar in den USA im Anschlagsjahr 2001 deutlich niedriger, als das Risiko, im Strassenverkehr zu sterben.[17] [18]

Vor dem Hintergrund dieser Ängste wird oftmals argumentiert, dass Überwachungsmassnahmen - selbst wenn keine Erfolge messbar sind - ein Sicherheitsgefühl schaffen. Einige wissenschaftliche Studien deuten

15 http://privacyfoundation.ch/de/service/anonymisierungsdienste/anonym-surfen-mit-tor.html

16 http://gnupg.org/index.de.html

17 http://www.washingtonpost.com/wp-dyn/content/article/2005/04/27/AR2005042702096.html

18 http://www-fars.nhtsa.dot.gov/Main/index.aspx

jedoch darauf hin, dass die Dauer des gewonnen Sicherheitsgefühls nur sehr kurzlebig ist.[19] [20] Es ist sogar eher ein gegenteiliger Effekt zu beobachten: je mehr der Staat gewisse Bereiche überwachen lässt und je mehr Überwachung in den Massenmedien verbreitet wird, desto mehr entsteht bei der Bevölkerung das Gefühl, dass besondere Gefahren in diesem Bereich lauern - die Unsicherheit wächst langfristig. Es ergibt sich somit durch Rückkopplung ein System, in dem immer mehr Überwachungsmassnahmen aufgrund des Unsicherheitsgefühls umgesetzt werden. Diese Spirale aus Überwachungsmassnahmen und «Unsicherheitsgefühlen» führt geradewegs in einen Überwachungsstaat.

19 http://wwz.unibas.ch/fileadmin/wwz/redaktion/wipo/Alois_Stutzer/faz1.pdf

20 http://onlinelibrary.wiley.com/doi/10.1111/j.1540-5907.2005.00144.x/full